

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

IN RE: SOCIAL MEDIA ADOLESCENT
ADDICTION/PERSONAL INJURY
PRODUCTS LIABILITY LITIGATION

Case No. 22-md-03047-YGR (TSH)

DISCOVERY ORDER

Re: Dkt. No. 271

With respect to a protective order in this action, we are down to three disputes. ECF No. 271.

A. Export Controls

Plaintiffs' proposed paragraph 12.8 states: "The Producing Party shall be responsible for identifying any technical data subject to laws or regulations that limit the export of technical data (including laws or regulations that limit the release of technical data to foreign persons or nationals in the United States or elsewhere). The Receiving Party shall take measures necessary to ensure compliance with any such export control laws or regulations. This provision does not apply to Protected Material designated 'HIGHLY CONFIDENTIAL (SOURCE CODE),' which shall be governed by a later order."

Defendants' proposed paragraph 12.8 states: "Except to the extent permitted by law and necessary for a litigation need, no Protected Material designated 'HIGHLY CONFIDENTIAL (COMPETITOR)' may leave the territorial boundaries of the United States of America, be viewed outside the territorial limits of the United States of America, or be made available to any foreign national who is not (i) lawfully admitted for permanent residence in the United States or (ii) identified as a protected individual under the Immigration and Naturalization Act (8 U.S.C.

1 1324b(a)(3)). At the time of production, a Disclosing Party will identify to the Receiving Party
 2 the Export Control Classification Numbers of the technical data contained in the Disclosing
 3 Party's 'HIGHLY CONFIDENTIAL (COMPETITOR)' productions to the best of its knowledge,
 4 and the Receiving Party must ensure that it complies with all applicable export control regulations.
 5 This provision does not apply to Protected Material designated 'HIGHLY CONFIDENTIAL
 6 (SOURCE CODE),' which shall be governed by a later order."

7 There are three sub-disputes here. One is whether Defendants must identify any technical
 8 data on a document-by-document basis that is subject to laws or regulations that limit the export of
 9 technical data. Defendants say this would be very burdensome because in their everyday business
 10 they do not designate export control information at the document level. Defendants state that
 11 requiring such designation at the document level for discovery purposes would require specialized
 12 and expensive manual review by an export controls expert and an engineer able to translate
 13 technical documents. Based on Defendants' representation that they do not ordinarily designate
 14 export control information at the document level, the Court will not require them to do so for
 15 document production purposes and will instead allow Defendants to use a reasonable proxy for
 16 documents that may be subject to export control.

17 The next sub-dispute is whether "Highly Confidential (Competitor)" Protected Material
 18 ("HCC") is a reasonable proxy for documents that may be subject to export control. The answer is
 19 no. Both sides propose that HCC be defined as "Protected Material the disclosure of which to
 20 another Party or Non-Party would create a substantial risk of serious harm that could not be
 21 avoided by less restrictive means." The focus of the HCC designation is therefore on
 22 competitively sensitive business information, which is not the focus of export control regulations.
 23 The Court is not going to impose export controls on, for example, emails that discuss confidential
 24 business plans. The parties appear to agree that export control regulations apply only to technical
 25 data. The Court concludes that the protective order needs a new defined term: "Export Control
 26 Protected Material: Highly Confidential (Competitor) Protected Material of a technical nature that
 27 may be subject to export control regulations." That term should then be used in Defendants'
 28 paragraph 12.8 in place of HCC.

1 Third, the Court agrees with Plaintiffs that the words “and necessary for a litigation need”
2 in Defendants’ paragraph 12.8 are unnecessary given the existing use restriction in paragraph 7.1.

3 Accordingly, the Court adopts Defendants’ proposed paragraph 12.8 as modified above.

4 **B. Definition of Expert**

5 As to the definition of an “expert,” Plaintiffs are moving backwards, which is dispiriting.
6 When we were last here, “Plaintiffs object[ed] to Defendants’ proposed definition of ‘Expert’ to
7 exclude any ‘past’ employee ‘of a Party or a Party’s competitor.’” ECF No. 192. Plaintiffs
8 prevailed, and the Court struck the ban on past employees of a party or a party’s competitor.
9 4/10/2023 Tr. at 31. Plaintiffs now raise a new dispute, saying they want to be able to retain a
10 current employee of a party’s competitor as an expert. Backsliding like this is the opposite of
11 what the Court expects from meeting and conferring.

12 On the merits, the Court does not agree with Plaintiffs’ proposal. Discovery in this MDL
13 proceeding is likely to involve highly confidential materials, and forcing a defendant to turn over
14 its highly confidential materials to a current employee of a competitor is too much to demand.
15 Plaintiffs argue that “Plaintiffs would be prevented from retaining a Microsoft coder who works
16 on the Windows operating system, or an Amazon engineer who works on cloud data storage, even
17 though such products have nothing to do with this case.” However, the Court is skeptical that
18 current employees of Microsoft or Amazon, or other competitors of Defendants, moonlight as
19 experts for Plaintiffs suing the tech industry. Experts typically work in firms, in academia, or by
20 themselves. Plaintiffs have not persuaded the Court that excluding current employees of
21 Defendants’ competitors inappropriately narrows the field of experts available to them.

22 **C. Disclosure of Experts**

23 Finally, Plaintiffs ask the Court to revisit its prior decision requiring expert disclosures
24 before a party may disclose protected material to an expert. The parties dispute what Judge Kuhl
25 said in a May 3, 2023 hearing in the JCCP proceeding.

26 The Court declines to change its mind. Defendants will be producing highly sensitive
27 documents in this MDL proceeding, and both sides agree that some of those materials will be
28 subject to export controls. Defendants are entitled to know who has their stuff. That can’t be the

1 subject of mystery. While the Court rejected Defendants' proposed data security provisions at the
2 April 10, 2023 hearing, that was not out of the belief that there is no problem to be addressed.
3 Data breaches and ransomware attacks are on the rise. Forcing Defendants to produce extremely
4 sensitive materials, and then telling them "Don't worry who has your data – that's not for you to
5 know" is really just too much. Under Plaintiffs' proposal, Defendants would never, not even at
6 the conclusion of litigation, know all the expert firms that have or had their data because they
7 would never learn about the experts Plaintiffs later decided not to use. If a data breach happens
8 and some of Defendants' highly confidential materials end up in the public record, Defendants
9 need to know all the possible sources of the breach.

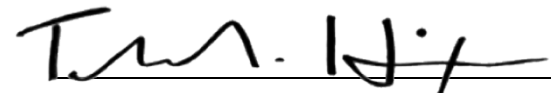
10 Further, the other purpose of the disclosure is to give the designating party the opportunity
11 to object if it believes its protected material should not be disclosed to a particular expert. Doing
12 away with the disclosure requirement would substantively abolish the opportunity to object. The
13 day expert reports are due is not when a designating party should learn for the first time that
14 someone who never should have had their protected materials has them.

15 **D. Next Step**

16 The Court **ORDERS** the parties to submit a proposed protective order in conformity with
17 this order.

18 **IT IS SO ORDERED.**

19
20 Dated: May 22, 2023



THOMAS S. HIXSON
United States Magistrate Judge